<u>**Listing of Claims:**</u>

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. - 8. (Canceled).

9. - 16. (Canceled).

17. - 154. (Canceled).

155. **(New)** A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

    a) storing recipient data pertaining to at least one party on a computer associated with said at least one party for purposes of retrieving e-mail, said stored recipient data identifying said at least one party;

    b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

    c) delivering said e-mail to a recipient e-mail address;

    d) detecting an access event, and discovering the stored recipient data that identifies the recipient associated with the recipient e-mail address to which such e-mail was delivered;

    e) generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice; and

    f) sending said confirmation of receipt notice, wherein the discovered recipient data contained in said confirmation of receipt notice can be compared to delivery information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

156. (New) The method as in claim 155, wherein said stored recipient data comprises a data file containing pre-recorded recipient data.

157. (New) The method as in claim 155, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

158. (New) The method as in claim 155, wherein said access event comprises access of an email account associated with said recipient e-mail address.

159. (New) The method as in claim 155, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

160. (New) The method as in claim 155, further comprising the steps of:

transmitting and delivering to the recipient e-mail address an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for discovering the stored recipient data, a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice,

and upon the detection of the access event, automatically executing the first, second, and third modules of the executable attachment file.

161. (New) The method as in claim 160, wherein the executable attachment file has a fourth module transmitted and delivered therewith, the fourth module for detecting the access event, and further comprising the step of:

automatically executing the fourth module upon delivery of the attachment file to the recipient e-mail address.

162. (New) The method as in claim 155, further comprising the step of determining, upon delivery of the e-mail file to the recipient e-mail address, whether the delivered e-mail file is of at least one designated file-type requiring a confirmation of receipt notice, and

wherein the detecting step is performed if it is determined that the delivered e-mail file is of the at least one designated file-type.

163. (New) The method as in claim 155, wherein said computer is a recipient computer.

164. (New) The method as in claim 163, wherein said recipient computer is a server of a service provider.

165. (New) The method as in claim 163, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

166. (New) The method as in claim 155, wherein said computer is a remote user computer from which said recipient may gain remote access to said recipient e-mail address.

167. (New) The method as in claim 155, wherein said stored recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

168. (New) The method as in claim 155, wherein said stored recipient data comprises, at least in part, identity information that identifies an individual.

- 4 -

169. (New) The method as in claim 168, wherein said identity information pertains to biometric identification.

170. (New) The method as in claim 169 further comprising means for recognizing biometric attributes of an individual.

171. (New) The method as in claim 168, wherein said identity information includes alphanumeric text identification information.

172. (New) The method as in claim 155, wherein said stored recipient data comprises, at least in part, information that identifies a business.

173. (New) The method as in claim 155, wherein said stored recipient data comprises, at least in part, information that identifies an organization.

174. (New) The method as in claim 155, wherein said stored recipient data comprises, at least in part, a computer generated user code.

175. (New) The method as in claim 155 further including the step of including in said confirmation of receipt notice access event data of attendant conditions of said access event.

176. (New) The method as in claim 155, wherein said party is an individual.

177. (New) The method as in claim 155, wherein said party is a business.

178. (New) The method as in claim 155, wherein said party is an organization.

179. (New) The method as in claim 155, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

180. (New) The method as in claim 155, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

181. (New) The method as in claim 155, wherein said recipient e-mail address is associated with a recipient computer.

182. (New) The method as in claim 181, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

183. (New) The method as in claim 181, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

184. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b) delivering said e-mail to a recipient e-mail address;

c) detecting an access event, and prompting the party who requested said access to enter recipient data prior to allowing the requested access, said recipient data identifying the party who requested said access;

d) generating a confirmation of receipt notice wherein the entered recipient data is included in said confirmation of receipt notice; and

- 6 -

e) sending said confirmation of receipt notice, wherein the entered recipient data contained in said confirmation of receipt notice can be compared to delivery information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

185. **(New)** The method as in claim 184, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

186. **(New)** The method as in claim 184, wherein said access event comprises access of an email account associated with said recipient e-mail address.

187. **(New)** The method as in claim 184, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

188. **(New)** The method as in claim 184, further comprising the steps of:

transmitting and delivering to the recipient e-mail address an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for prompting the party who requested said access event to enter recipient data, a second module for generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice; and

upon the detection of the access event, automatically executing the first, second, and third modules of the executable attachment file.

189. **(New)** The method as in claim 188, wherein the executable attachment file has a fourth module transmitted and delivered therewith, the fourth module for detecting the access event, and further comprising the step of automatically executing the fourth module upon delivery of the attachment file to the recipient e-mail address.

190. (New) The method as in claim 184, further comprising the step of determining, upon delivery of the e-mail file to the recipient e-mail address, whether the delivered e-mail file is of at least one designated file-type requiring a confirmation of receipt notice, and

wherein the step of prompting said party who requested said access event for recipient data is performed if it is determined that the delivered e-mail file is of the at least one designated file-type.

191. (New) The method as in claim 184, wherein said recipient e-mail address is associated with a recipient computer.

192. (New) The method as in claim 191, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

193. (New) The method as in claim 191, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

194. (New) The method as in claim 184, wherein said entered recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

195. (New) The method as in claim 184, wherein said entered recipient data comprises, at least in part, identity information that identifies an individual.

196. (New) The method as in claim 195, wherein said identity information pertains to biometric identification.

197. (New) The method as in claim 196 further comprising means for recognizing biometric attributes of an individual.

198. (New) The method as in claim 195, wherein said identity information includes alphanumeric text identification information.

199. (New) The method as in claim 184, wherein said entered recipient data comprises, at least in part, information that identifies a business.

200. (New) The method as in claim 184, wherein said entered recipient data comprises, at least in part, information that identifies an organization.

201. (New) The method as in claim 184, wherein said entered recipient data comprises, at least in part, a computer generated user code.

202. (New) The method as in claim 184 further including the step of including in said confirmation of receipt notice access event data of attendant conditions of said access event.

203. (New) The method as in claim 184, wherein said party is an individual.

204. (New) The method as in claim 184, wherein said party is a business.

205. (New) The method as in claim 184, wherein said party is an organization.

206. (New) The method as in claim 184, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

207. (New) The method as in claim 184, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

208. (New) A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

   a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

   b) delivering said e-mail to a recipient e-mail address;

   c) acquiring recipient data that is related to biometric identification of the recipient;

   d) detecting an access event, and generating a confirmation of receipt notice wherein the acquired recipient data is included in said confirmation of receipt notice; and

   e) sending said confirmation of receipt notice.

209. (New) The method as in claim 208, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

210. (New) The method as in claim 208, wherein said access event comprises access of an email account associated with said recipient e-mail address.

211. (New) The method as in claim 208, wherein said access event comprises activation of e-mail processing software associated with said recipient e-mail address.

212. (New) The method as in claim 208, further comprising the step of:

   transmitting and delivering to the recipient e-mail address an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for acquiring recipient data that is related to biometric identification of the recipient, a second module for

- 10 -

generating the confirmation of receipt notice, and a third module for transmitting the confirmation of receipt notice; and

upon the detection of the access event, automatically executing at least the second and third modules of the executable attachment file.

213.　(New) The method as in claim 212, wherein the executable attachment file has a fourth module transmitted and delivered therewith, the fourth module for detecting the access event, and further comprising the step of:

automatically executing the fourth module upon delivery of the attachment file to the recipient e-mail address.

214.　(New) The method as in claim 208,

further comprising the step of determining, upon delivery of the e-mail file to the recipient e-mail address, whether the delivered e-mail file is of at least one designated file-type requiring a confirmation of receipt notice, and

wherein the step of prompting said party who initiated said access event for recipient data occurs upon a determination that the delivered e-mail file is of the at least one designated file-type.

215.　(New) The method as in claim 208, wherein said recipient e-mail address is associated with a recipient computer.

216.　(New) The method as in claim 215, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

217.　(New) The method as in claim 215, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software

- 11 -

and being capable of receiving e-mail.

218. **(New)** The method as in claim 208, wherein said acquired recipient data is further related to alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

219. **(New)** The method as in claim 208, wherein said acquired recipient data comprises identity information that identifies an individual.

220. **(New)** The method as in claim 208 further comprising means for recognizing biometric attributes of an individual.

221. **(New)** The method as in claim 208, wherein said acquired recipient data comprises information that identifies a business.

222. **(New)** The method as in claim 208, wherein said acquired recipient data comprises information that identifies an organization.

223. **(New)** The method as in claim 208, wherein said acquired recipient data comprises a computer generated user code.

224. **(New)** The method as in claim 208 further including the step of including in said confirmation of receipt notice access event data of attendant conditions of said access event.

225. **(New)** The method as in claim 208, wherein said recipient is an individual.

226. **(New)** The method as in claim 208, wherein said recipient is a business.

227. **(New)** The method as in claim 208, wherein said recipient is an organization.

228. **(New)** The method as in claim 208, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

229. **(New)** The method as in claim 208, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

230. **(New)** The method as in claim 208, wherein said recipient data is acquired prior to said access event.

231. **(New)** The method as in claim 208, wherein said recipient data is acquired as a requisite condition for permitting access to said delivered e-mail.

232. **(New)** The method as in claim 208, wherein said recipient data is acquired as a requisite condition for permitting access to said recipient e-mail address.

233. **(New)** The method as in claim 208, wherein said recipient data is acquired as a requisite condition for operating a remote user computer, said remote user computer being operable to gain access to said recipient e-mail address.

234. **(New)** The method as in claim 208, wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

- 13 -

235. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

    a) storing recipient data on a computer associated with e-mail retrieval, said stored recipient data identifying a particular party;

    b) transmitting an e-mail from a sender computer to the intended recipient, the sender computer being connected to a communications network;

    c) delivering said e-mail to a recipient e-mail address;

    d) detecting an access event, and discovering the stored recipient data that identifies the party associated with the recipient e-mail address to which such email was delivered;

    e) generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice; and

    f) sending said confirmation of receipt notice.

236. (New) A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

    a) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

    b) delivering said e-mail to a recipient e-mail address;

    c) detecting an access event, and prompting the party associated with said access event to enter recipient data prior to allowing the requested access, said recipient data identifying the party associated with said requested access;

    d) generating a confirmation of receipt notice wherein the entered recipient data is included in said confirmation of receipt notice; and

    e) sending said confirmation of receipt notice.

237.   (New) A method for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a)   transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

b)   delivering said e-mail to a recipient e-mail address;

c)   identifying said recipient via biometric identification;

d)   detecting an access event, and generating a confirmation of receipt notice wherein data that identifies said recipient is included in said confirmation of receipt notice; and

e)   sending said confirmation of receipt notice.

238.   (New) The method as in claim 237, wherein said data that identifies said recipient is related to alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239.   (New) The method as in claim 237, wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

240.   (New) The method as in claim 237 further comprising means for recognizing biometric attributes of an individual.

241.   (New) The method as in claim 237, wherein said data that identifies said recipient comprises identity information that identifies an individual.

242. (New) The method as in claim 237, wherein said data that identifies said recipient comprises information that identifies a business.

243. (New) The method as in claim 237, wherein said data that identifies said recipient comprises information that identifies an organization.

244. (New) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) recipient data stored on a computer associated with the intended recipient, said stored recipient data associated with a particular recipient e-mail address and identifying a party associated with said particular e-mail address;

d) software capable of detecting an access event, wherein, upon detecting said access event, said software executes the steps of:

i.   retrieving the stored recipient data that identifies the party associated with said particular recipient e-mail address to which such email was delivered; and

ii.   including the acquired recipient data in a confirmation of receipt notice; and

e) means for transmitting said confirmation of receipt notice to an e-mail address associated with said sending party.

245. (New) The system as in claim 244, wherein said access event comprises access of a delivered e-mail.

- 16 -

246. (New) The system as in claim 244, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

247. (New) The system as in claim 244, wherein said access event comprises activation of the e-mail processing software associated with the e-mail address to which said e-mail was delivered.

248. (New) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) software capable of detecting an access event, wherein, upon detecting said access event, said software:

    i. prompts the party associated with said access event to enter recipient data prior to allowing the requested access, if no such recipient data pertaining to said party has been entered prior to said access event, said recipient data identifying the party associated with said requested access; and

    ii. includes the acquired recipient data in a confirmation of receipt notice; and

e) means for transmitting said confirmation of receipt notice to an e-mail address associated with said sending party.

249. (New) The system as in claim 248, wherein said access event comprises access of a delivered e-mail.

- 17 -

250. (New) The system as in claim 248, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

251. (New) The system as in claim 248, wherein said access event comprises activation of the e-mail processing software associated with the e-mail address to which said e-mail was delivered.

252. (New) A system for verifying whether e-mail sent by a sending party was accessed by an intended recipient, said system comprising:

a) a sender computer connected to a communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer being capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) biometric identification means for recognizing biometric attributes of an individual;

d) software capable of detecting an access event, said software also being capable of acquiring biometric data identifying the party causing said access event, and including the acquired data in a confirmation of receipt notice; and

e) means for transmitting said confirmation of receipt notice to an e-mail address associated with said sending party.

253. (New) The system as in claim 252, wherein said access event comprises access of a delivered e-mail.

254. (New) The system as in claim 252, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

255. (New) The system as in claim 252, wherein said access event comprises activation of the e-mail processing software associated with the e-mail address to which said e-mail was delivered.